

**Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, DC 20554**

Rules and Regulations Implementing the        )        WC Docket No. 11-39  
Truth in Caller ID Act of 2009                )

**COMMENTS OF AT&T INC.**

AT&T Inc. (“AT&T”), on behalf of its operating company subsidiaries, hereby files these comments in response to the Notice of Proposed Rulemaking (“NPRM”) in the aforementioned docket.

The Truth in Caller ID Act of 2009 (“Act”) prohibits persons or entities from using caller identification services in connection with any telecommunications service or IP-enabled voice service to transmit misleading or inaccurate caller identification information (“Caller ID”) with the intent to defraud, cause harm, or wrongfully obtain anything of value (hereinafter “spoofing”).<sup>1</sup> AT&T fully supports the adoption of targeted rules to thwart spoofing. As a provider of Caller ID services and telecommunications and IP-enabled voice services to millions of consumers, AT&T has received an increasing number of customer inquiries and complaints regarding spoofing, and often is the first stop in assisting customers and law enforcement in determining the origination of spoofed calls, and ultimately the identity of the calling parties.<sup>2</sup>

---

<sup>1</sup> The Truth in Caller ID Act of 2009 states, “It shall be unlawful for any person within the United States, in connection with any telecommunications service or IP-enabled voice service, to cause any caller identification service to knowingly transmit misleading or inaccurate caller identification information with the intent to defraud, cause harm or wrongfully obtain anything of value, unless such transmission is exempted pursuant to paragraph 3(B).”

<sup>2</sup> Customers and law enforcement rely on AT&T to investigate spoofing because, as the provider of Caller ID services to end users, AT&T receives whatever CPN and ANI data is transmitted for spoofed calls. CPN, or Calling Party number, “refers to the subscriber line number or the directory number contained in the calling parameter of the call set-up message associated with an interstate call on a Signaling System 7 network.” 47 C.F.R. §64.1600(c). The CPN generally is the number displayed on Caller ID devices. ANI “refers to the delivery of the calling party’s billing number by a local exchange carrier to any

Based on AT&T's experience in investigating spoofing, it is abundantly clear that persons or entities engaging in such conduct will use every available means to deceive the called party without detection. Absent robust anti-spoofing regulations, and enforcement thereof, spoofing will continue unabated.

In crafting its regulations, the Commission should ensure that its anti-spoofing regulations are technology neutral and thus apply to all spoofing activity in connection with any telecommunications or IP-enabled voice service.<sup>3</sup> Additionally, the Commission should ensure that certain activities are exempt from the anti-spoofing regulations, specifically: (1) the manipulation of Caller ID to investigate fraud, or for telemarketing or customer service purposes; and (2) the mere transmission, by a telecommunications carrier or IP-enabled voice service provider, of Caller ID received from a customer or another carrier or provider. Such activities are for legitimate reasons and in no way are intended to defraud, cause harm or wrongfully obtain something of value. Additionally, the Commission should ensure that its anti-spoofing regulations apply to any telecommunications carrier or IP-enabled voice service provider that manipulates ANI, including Charge number, to avoid, or reduce the payment of, access charges.

**1. AT&T generally supports the Commission's anti-spoofing regulations, but offers a few recommendations to its associated definitions.**

---

interconnecting carrier for billing or routing purposes, and the subsequent delivery of such number to end users." 47 C.F.R. § 64.1600(b). The ANI is necessary for the billing and routing of calls. In many instances, the CPN and ANI are the same. To the extent the calling party has triggered Caller ID blocking for the call, AT&T will honor the privacy election.

<sup>3</sup> AT&T recognizes that not all current transmission technologies are covered by the Act. To prevent regulatory arbitrage, AT&T urges the Commission to recommend in its report to Congress that the Act be amended to prohibit spoofing in connection with *any* transmission service.

In the NPRM, the Commission seeks comment on its proposed prohibition on spoofing as well as key, associated definitions. AT&T provides its comments below.

*Anti-spoofing regulation:* The Commission proposes to adopt the following anti-spoofing regulation:

No person or entity in the United States shall with the intent to defraud, cause harm or wrongfully obtain anything of value, knowingly cause directly or indirectly any caller identification service to transmit or display misleading or inaccurate caller identification information<sup>4</sup>

AT&T fully supports the proposed regulation. In its implementing order, the Commission should make clear that this rule is purposely broad and intended to cover not only the person or entity initiating a spoofed call, but also any company that provides a service that allows a calling party to manipulate Caller ID where that company (1) is aware, or should have been aware, that the calling party is engaging in fraudulent, deceptive, or harmful behavior, and (2) facilitates the spoofed call.<sup>5</sup> Application of the prohibition to such companies is essential to curb spoofing. While AT&T recognizes that a company offering such services may not have initiated a spoofed call, once it becomes aware that a caller is using its services to engage in such unscrupulous conduct, such a company would, at a minimum, be engaged in facilitation of spoofing, and thus would fall within the scope of the prohibition against “knowingly” causing “directly or indirectly” its Caller ID service to transmit misleading or inaccurate Caller ID. Because it is often very difficult to determine the party originating a spoofed call (as these parties will try and hide behind the provider of the spoofing services), it is essential that the Commission’s rules

---

<sup>4</sup> 47 U.S.C. § 227(e)(1). Subsection (5) sets forth the civil forfeiture penalties for spoofing.

<sup>5</sup> See Section 3(a), *infra*. Telecommunications carriers and IP-enabled voice service providers that merely transmit Caller ID they receive from their customers or other telecommunications carriers or IP-enabled voice service providers, should be exempt.

apply to those companies that facilitate spoofing by knowingly providing (or continuing to provide) services that allow calling parties to manipulate Caller ID to engage in spoofing. Sanctioning companies that do so would encourage them to take reasonable steps to ensure that their Caller ID manipulation services are used only for legitimate purposes.

*Caller ID and Caller ID Service Definitions:* The proposed anti-spoofing regulation includes the terms “Caller ID” and “Caller ID Service.” The Commission proposes to adopt the definitions of these terms as set forth in the Act, with the exception of changing the term “IP-enabled voice service” in those definitions to “interconnected VoIP service.”<sup>6</sup>

The Commission should revise both definitions to replace the term “interconnected VoIP service” with “IP-enabled voice service.” The Act prohibits spoofing in connection with any telecommunications service or IP-enabled voice service and then defines the term “IP-enabled voice service” to have the meaning set forth in Section 9.3 of the Commission’s rules, which the Commission may amend from time to time. Currently, that section includes a definition of Interconnected VoIP service only. Because spoofing is technology neutral and may evolve over time to include other IP-enabled voice services, there simply is no rational basis for locking-in the anti-spoofing rules only to interconnected VoIP services. Distinguishing between interconnected and non-interconnected VoIP services, for example, would allow persons or entities that choose to use allegedly non-interconnected IP-enabled voice services, such as Skype and Google Voice, to engage in spoofing without repercussion — a result plainly at odds with

---

<sup>6</sup> The NPRM proposes the following definitions:

Caller identification information. The term “Caller identification information” means information provided by a caller identification service regarding the telephone number or, or other information regarding the origination of, a call made using a telecommunications service or interconnected VoIP service.

Caller identification service. The term “Caller identification service” means any service or device designed to provide the user of the service or device with the telephone number of, or other information regarding the origination of, a call made using a telecommunications service or interconnected VoIP service. Such term includes automatic number identification services.

the goals of the Act. While AT&T does not offer a specific proposal for revising Section 9.3, it urges the Commission to amend that section as well as its definition of Caller ID and Caller ID service to ensure that spoofing in connection with *any* VoIP service is subject to its anti-spoofing regulations.

The Commission should also insert the following language in the definition of Caller ID: “...or other information regarding the origination *or routing or billing* of, ...” While the Act and the Commission’s proposed definition of “Caller ID service” includes ANI services, the proposed definition of “Caller ID” does not clearly refer to ANI-specific information, i.e. information regarding the routing or billing of a call. While CPN and ANI are often the same, in many instances they differ. Amending the definition of “Caller identification information” as AT&T proposes would remove any ambiguity as to whether the anti-spoofing regulations apply to ANI information, where it differs from CPN.

*CPN, ANI and Charge Number.* The Commission should also amend its current definitions of CPN, ANI and Charge number.<sup>7</sup> These definitions specifically refer to either the delivery of the billing number to interconnecting carriers by a local exchange carrier or the use of SS7 signaling technology. As currently codified, these definitions could limit the Caller ID subject to the anti-spoofing regulations, particularly where spoofing occurs in connection with IP-enabled voice services that do not involve local exchange carriers in the call path or SS7 signaling. The Commission should broaden its definition of CPN, ANI and Charge number to include telephone number and billing information transmitted by IP-enabled voice service providers via any available signaling technology.<sup>8</sup> This will ensure that all information provided by a Caller ID service to terminating carriers or IP-enabled voice service providers is covered by

---

<sup>7</sup> See fn.1-2, *supra*.

<sup>8</sup> The Commission should also consider making Charge Number a subset of ANI. Both are used for the proper billing and routing of calls, but the former is based on SS7 signaling.

the anti-spoofing regulations, regardless of the signaling technology (e.g. MF signaling, SS7 signaling, or SIP signaling) used, or carrier or provider in the call path.

- 2. The Commission should ensure that its anti-spoofing regulations apply to entities that manipulate ANI or Charge number to avoid, or reduce their payment of, access charges.**

By including ANI services in the definition of Caller ID service, Congress clearly intended the anti-spoofing regulations to apply to the fraudulent manipulation of ANI information. Without question, carriers or other entities that manipulate ANI or Charge number data to avoid or reduce their payment of access charges are intentionally engaging in fraudulent and deceptive behavior for the sole purpose of wrongfully obtaining a financial benefit.<sup>9</sup> The financial benefit, in fact, can be quite substantial where there is a wide disparity between interstate and intrastate access charges. AT&T has been and is involved in multiple investigations involving this type of fraudulent activity. While AT&T recognizes that the Commission is evaluating these issues in the Intercarrier Compensation (“ICC”) reform proceeding,<sup>10</sup> given the broad scope of the Act, the Commission could address this unscrupulous conduct through its anti-spoofing regulations as well as any regulations it adopts in that proceeding. AT&T thus urges the Commission to find that the manipulation of ANI (including Charge number) to avoid or reduce the payment of access charges is subject to the anti-spoofing regulations and any other regulations or penalties it may adopt in the ICC proceeding.

---

<sup>9</sup> In many instances, the CPN and ANI are not the same. In AT&T’s experience, some carriers or customers making interstate calls manipulate the ANI to reflect a local number to avoid paying access charges. Additionally, some carriers manipulate the charge number for the same result.

<sup>10</sup> *Developing an Unified Intercarrier Compensation Regime*, CC Docket No. 96-45, Notice of Proposed Rulemaking, ¶¶623-633 (rel. Feb. 2011).

**3. The Commission should exempt certain business activities from the anti-spoofing regulations.**

In the NPRM, the Commission proposes to adopt the two exemptions specified in the Act<sup>11</sup> and seeks comment on whether it should adopt any other exemptions. AT&T supports the adoption of those exemptions and encourages the Commission to adopt other exemptions, as detailed below.

- a. Telecommunications carriers or IP-enabled voice service providers that merely transmit Caller ID they receive from their customers or other telecommunications carriers or IP-enabled voice service providers should be exempt.**

Telecommunications carriers or IP-enabled voice providers that merely transmit Caller ID received from their customers or other providers<sup>12</sup> are not the culprits. These carriers and providers often have no way of determining whether any manipulated Caller ID they receive is for legitimate reasons, and further, often cannot even determine if the Caller ID was changed. By contrast, those companies whose primary business is offering Caller ID manipulation services, and who know, or should know, that a caller has requested Caller ID manipulation for fraudulent or harmful reasons, should be targeted by anti-spoofing regulations. Because many customers (specifically the called parties) mistakenly believe that AT&T and other

---

<sup>11</sup> The Commission proposes to adopt the following exemptions:

Paragraph (a) of this section shall not apply to:

- (1) Lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States; or
- (2) Activity engaged in pursuant to a court order that specifically authorizes the use of caller identification manipulation

<sup>12</sup> Telecommunications carriers are required to pass CPN for every interstate call. See 47 C.F.R. §64.1601.

telecommunications providers or IP-enabled voice service providers have some role in Caller ID manipulation because they transmit the Caller ID with the communications service, an exemption is necessary to remove any ambiguity in this regard.

**b. The Commission should exempt Caller ID manipulation for legitimate business reasons.**

There are legitimate business reasons for manipulating Caller ID. AT&T, for example, may manipulate Caller ID with various test equipment to emulate the customer experience when trouble shooting network issues. AT&T may manipulate Caller ID while investigating fraudulent uses of its network, including spoofing, and in this regard, may perform “test calls” using manipulated Caller ID to determine if spoofing (or other fraudulent activity) has or is occurring. While the exemptions in the Act would allow AT&T to perform such activities in conjunction with a court order or request from law enforcement, AT&T should have the flexibility to investigate spoofing in the absence of such orders or requests.<sup>13</sup> This would allow carriers to identify and stop — to the extent feasible — such fraudulent practices in a timely and efficient manner.

AT&T also engages in a variety of telemarketing campaigns and customer service calls, and in such instances, will change the CPN to reflect the best contact telephone number — out of the thousands of telephone numbers assigned to AT&T — for customers to reach AT&T. Any called party that dials the CPN provided will have the ability to identify AT&T as the caller, to determine the reason for the call and to make a do-not-call request (where appropriate) — notably, all key requirements AT&T must adhere to under the Commission’s telemarketing

---

<sup>13</sup> The FCC has, for example, permitted carriers to use CPNI without customer approval to protect their networks and to protect their customers from fraudulent use of their services. See 47 C.F.R. § 64.2005(d).

rules.<sup>14</sup> These Caller ID manipulation activities are clearly for legitimate business reasons, and in no way are fraudulent, deceptive or harmful to the called party. The Commission should therefore make clear that Caller ID manipulation for legitimate business reasons is exempt.

## CONCLUSION

For the foregoing reasons, the Commission should adopt the anti-spoofing regulations and associated definitions and exemptions as proposed herein.

Respectfully Submitted,

/s/ Davida Grant

Davida Grant  
Gary Phillips  
Paul K. Mancini

AT&T Inc.  
1120 20<sup>th</sup> Street NW  
Suite 1000  
Washington, D.C. 20036  
(202) 457-3045 – phone  
(202) 457-3073 – facsimile

April 18, 2011

---

<sup>14</sup> 47 C.F.R. § 64.1200(a)(6), (b)(1).